

In the Claims:

Please replace the pending claims 1-57 with those set forth below, in which claims 1, 10, 15, 18, 19, 21, 35, 39, 42-44, 46-48, and 50 are amended and claims 2, 6-8, 11, 13-14, 16, 20, 22, 24-25, 28-34, and 52-57 are canceled without prejudice.

1-34. (Canceled)

35. (Currently Amended) A home control system that uses electrical power lines for communications, comprising:

a plurality of components that are connected for communications among themselves through the electrical power lines, wherein the communications among the plurality of components is established through a single communication protocol;

a sending one of the components being configured to send messages over the electrical power lines in accordance with [[steps]] acts comprising:

calculating a first message authentication code based on a predefined one-way function of data from a message and of a key value that is shared between sending and receiving components;

1 including the message authentication code in the
2 message;

3 sending the message over the electrical power lines;
4 a receiving one of the components being configured to receive
5 messages in accordance with [[steps]] acts comprising:

6 receiving a message over the electrical power lines;
7 calculating a second message authentication code
8 based on the predefined one-way function of the data from the message and of the
9 a current shared key value;
10

11 concluding that the message is either not authentic or
12 contains a data error if the first and second message authentication codes do not
13 match.
14

15
16 36. (Original) A home control system as recited in claim 35, wherein
17 the shared key value is from a sequence of key values;

18 the sending component being further configured to change
19 from a current to a subsequent key value in the sequence without notifying the
20 receiving component;
21

22 the receiving component being further configured to calculate
23 a third message authentication code based on the predefined one-way function of
24 the data from the message and of the subsequent key value;
25

1 the receiving being further configured to change from the
2 current key value to the subsequent key value if the first and second message
3 authentication codes do not match but the first and third message authentication
4 codes do match.

5
6
7 37. (Original) A home control system as recited in claim 35, wherein
8 the shared key value is from a sequence of key values;

9 the sending component being further configured to change
10 from a current to a subsequent key value in the sequence without notifying the
11 receiving component;

12 the receiving component being further configured to calculate
13 a third message authentication code based on the predefined one-way function of
14 the data from the message and of the subsequent key value;

15 the receiving being further configured to change from the
16 current key value to the subsequent key value if the first and second message
17 authentication codes do not match but the first and third message authentication
18 codes do match;

19 wherein the sending and receiving components calculate the
20 sequence of key values using a one-way function of a counter value that advances
21 to generate each sequential key value.
22
23
24
25

38. (Original) A home control system as recited in claim 35, wherein the shared key value is from a sequence of key values, and wherein the sending and receiving components calculate the sequence of key values using a one-way function of counter values that advance to generate each sequential key value.

39. (Currently Amended) ~~[[A]]~~ An electrical component that is connected for communications with other electrical components of a particular group using electrical power lines in a building, comprising:

a processor;

a transmitter that is responsive to the processor to send data using the electrical power lines;

the processor being programmed to compose and send messages in conjunction with the transmitter, each message including a message authentication code based on a predefined one-way function of data from the message and of a key value that is shared between a plurality of components;

wherein the communications with other electrical components of the particular group is established through a single communication protocol.

40. (Original) An electrical component as recited in claim 39, wherein the shared key value is from a sequence of key values, the processor being

1 further programmed to change from a current to a subsequent key value in the
2 sequence without notifying a receiving component.

3
4 41. (Original) An electrical component as recited in claim 39,
5 wherein the shared key value is from a sequence of key values, wherein the
6 processor calculates the sequence of key values using a one-way function of a
7 counter values that advance to generate each sequential key value.
8

9
10 42. (Currently Amended) [[A]] An electrical component that is
11 connected for communications with other electrical components of a particular
12 group using electrical power lines in a building, comprising:

13 a processor;

14
15 a receiver that functions in conjunction with the processor to
16 receive messages from other electrical components using the electrical power
17 lines, such messages including first message authentication codes;

18 the processor being programmed to calculate a second
19 message authentication code for each message based on a predefined one-way
20 function of the data from the message and of a key value that is shared between a
21 plurality of components;
22

23 the processor being further programmed to compare the first
24 and second message authentication codes to authenticate each message;
25

1 wherein the communications with other electrical components
2 of the particular group is established through a single communication protocol.
3

4 43. (Currently Amended) An electrical component as recited in
5 claim 42, wherein the shared key value is from a sequence of key values, the
6 processor programmed to perform the following [[steps]] operations:
7

8 calculating a third message authentication code based on the
9 predefined one-way function of the data from the message and of a subsequent key
10 value in the sequence of key values;

11 further comparing the first and third message authentication
12 codes to authenticate each message.

13 changing from the current key value to the subsequent key
14 value if the first and second message authentication codes do not match but the
15 first and third message authentication codes do match.
16

17
18 44. (Currently Amended) An electrical component as recited in
19 claim 42, wherein the shared key value is from a sequence of key values, the
20 processor programmed to perform the following [[steps]]:
21

22 calculating the sequence of key values using a one-way
23 function of a counter value that advances to generate each sequential key value;
24
25

calculating a third message authentication code based on the predefined one-way function of the data from the message and of a subsequent key value in the sequence of key values;

further comparing the first and third message authentication codes to authenticate each message [.] ;

changing from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match.

45. (Original) An electrical component as recited in claim 42, wherein the shared key value is from a sequence of key values, wherein the processor calculates the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value.

46. (Currently Amended) A method of communicating electronically between a plurality of electrical components using electrical power lines in a building, the method comprising the following steps:

designating groups of the electrical components that communicate among themselves;

sharing a key value between components of a particular group;

1 calculating a first message authentication code based on a
2 predefined one-way function of data from a message and of the key value that is
3 shared by components of the particular group;

4 including the message authentication code in the message;

5 sending the message over the electrical power lines;

6 receiving the message;

7 calculating a second message authentication code based on
8 the predefined one-way function of the data from the message and of the shared
9 key value; and

11 comparing the first and second message authentication codes
12 to authenticate each message;

13 wherein the electronic communication between the electrical
14 components is established through a single communication protocol.
15

16
17 47. (Currently Amended) A method as recited in claim 46, wherein
18 the shared key value is from a sequence of key values, the method further
19 comprising an additional [[step]] act of changing from a current to a subsequent
20 key value in the sequence without notifying receiving components.
21
22
23
24
25

1 48. (Currently Amended) A method as recited in claim 46, wherein
2 the shared key value is from a sequence of key values, the method further
3 comprising:

4 calculating a third message authentication code based on the
5 predefined one-way function of the data from the message and of a subsequent key
6 value in the sequence of key values;

7 further comparing the first and third message authentication
8 codes to authenticate each message [.] ;

9 changing from the current key value to the subsequent key
10 value if the first and second message authentication codes do not match but the
11 first and third message authentication codes do match.
12
13

14
15 49. (Original) A method as recited in claim 46, wherein the shared
16 key value is from a sequence of key values, the method further comprising:

17 calculating the sequence of key values using a one-way
18 function of a counter value that advances to generate each sequential key value;

19 calculating a third message authentication code based on the
20 predefined one-way function of the data from the message and of a subsequent key
21 value in the sequence of key values;

22 further comparing the first and third message authentication
23 codes to authenticate each message;
24
25

changing from the current key value to the subsequent key value if the first and second message authentication codes do not match but the first and third message authentication codes do match.

50. (Currently Amended) A method component as recited in claim 46, wherein the shared key value is from a sequence of key values, further comprising ~~a step of~~ calculating the sequence of key values using a one-way function of a counter value that advances to generate each sequential key value.

51. (Original) A method as recited in claim 46, further comprising:
assigning different group identifier codes to different groups of components;
specifying the group identifier code of an individual group in messages sent to components of said individual group;
determining whether a particular message is intended for a particular component by checking whether the group identifier code of the particular message matches the group identifier code of the particular component's group.

52-57. (Canceled)